

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 16 of 27

Remarks

The present amendment replies to a Non-Final Office Action dated January 4, 2005. Claims 1-39 as originally filed are currently pending in the present application. Claims 1, 4, 10, 11, 13, 14, 16, 17, 19, 20, 21, 23, 25, 27, 29, 31, 34, and 37 have been amended herein. Claim 1 has been amended to incorporate all the elements of claim 3 and claim 3 has been cancelled. In the Non-Final Office Action, the Examiner rejected pending claims 1-39 on various grounds. The Applicants respond to each ground of rejection as subsequently recited herein and respectfully request reconsideration and further examination of the present application.

- A. Claim 20 was rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

Claim 20 has been amended to change the typographical error "16" to "19." Withdrawal of the rejection of claim 20 under 35 U.S.C. §112, second paragraph, is respectfully requested.

- B. Claims 1-4 and 6-8 were rejected under 35 U.S.C. §102(b), as being anticipated by U.S. Patent No. 5,559,889 to Easter *et al.*

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the . . . claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 17 of 27

The Applicants have thoroughly considered the Examiner's remarks concerning patentability of claims 1-4 and 6-8 over U.S. Patent No. 5,559,889 to Easter *et al.* (the "*Easter* patent"). The Applicants have also thoroughly read the *Easter* patent. The Applicants assert that the *Easter* patent fails to disclose, teach, or suggest:

a method for configuring a semiconductor chip wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship; and embedding the private cryptographic key, the public cryptographic key, and the serial number in a read-only memory on the semiconductor chip, as recited in amended independent claim 1; or

an article of manufacture including a second read-only memory structure containing an embedded public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship, as recited in independent claim 6.

The *Easter* patent discloses designating a private key/public key pair for the IC chip. Fuse array 51 is encoded with the private key. Further, the fuse array is encoded with the hash value for the corresponding public key and a serial number. *See* column 5, lines 39-44. The *Easter* patent fails to disclose embedding a public cryptographic key, as recited in amended independent claims 1 and independent claim 6. The hash value is not unique to a specific public key and may correspond to a number of public keys. Further, the public cryptographic key and the private cryptographic key in the *Easter* patent are related by a cryptographic key pair relationship. *See* column 5, lines 39-40. The Applicants respectfully assert that the Examiner is mistaken in stating that because the public and private keys are different, they are not related by a cryptographic key pair relationship. The public and private keys must always be different, so the conclusion does not follow. Therefore, the *Easter* patent fails to disclose a public cryptographic key and a private cryptographic key that are not related by a cryptographic key pair relationship, as recited in amended independent claim 1 and independent claim 6.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 18 of 27

Claims 2 and 4, as well as claims 7 and 8 depend directly or indirectly from amended independent claim 1 and independent claim 6, respectively. Therefore, dependent claims 2, 4, 7, and 8 include all the elements and limitations of their respective independent claims. The Applicants respectfully submit that dependent claims 2, 4, 7, and 8 are allowable over the *Easter* patent for at least the same reason as set forth above with respect to their respective independent claims.

Withdrawal of the rejection of claims 1, 2, 4, and 6-8 under 35 U.S.C. §102(b) as being anticipated by the *Easter* patent is respectfully requested.

C. Claims 1, 5, 10, 13, and 16 were rejected under 35 U.S.C. §102(b), as being anticipated by U.S. Patent No. 5,787,172 to *Arnold*.

The Applicants have thoroughly considered the Examiner's remarks concerning patentability of claims 1, 5, 10, 13, and 16 over U.S. Patent No. 5,787,172 to *Arnold* (the "*Arnold* patent"). The Applicants have also thoroughly read the *Arnold* patent. The Applicants assert that the *Arnold* patent fails to disclose, teach, or suggest:

a method for configuring a semiconductor chip having an associated serial number including embedding the private cryptographic key, the public cryptographic key, and the serial number in a read-only memory on the semiconductor chip, selecting a public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship, as recited in amended independent claim 1; or

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 19 of 27

a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including a read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a cryptographic key pair relationship, the embedded client private key being associated with a client public key stored exclusively outside the client, as recited in amended independent claims 10, 13, or 16, respectively.

The *Arnold* patent discloses providing the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit, but fails to disclose embedding the serial number in a read-only memory on the semiconductor chip, as recited in amended independent claim 1. The *Arnold* patent also fails to disclose the embedded client private key being associated with a client public key stored exclusively outside the read-only memory structure, as recited in amended independent claims 10, 13, or 16. See column 4, lines 18-27.

Claim 5 depends directly from amended independent claim 1. Therefore, the dependent claim 1 includes all the elements and limitations of the respective independent claim. The Applicants respectfully submit that dependent claim 1 is allowable over the *Arnold* patent for at least the same reason as set forth above with respect to amended independent claim 1.

Withdrawal of the rejection of claims 1, 5, 10, 13, and 16 under 35 U.S.C. §102(b) as being anticipated by the *Arnold* patent is respectfully requested.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 20 of 27

- D. Claim 9 was rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,559,889 to Easter *et al.* in view of ecommerce-guide.com ("A Framework For SmartCard Payment Systems - Part One" by Mark Merkow, June 22, 2000).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references when combined must teach or suggest all the claim limitations. See MPEP 2143.

Claim 9 was rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,559,889 to Easter *et al.* (the "*Easter* patent") in view of ecommerce-guide.com ("A Framework For SmartCard Payment Systems - Part One" by Mark Merkow, June 22, 2000) (the "*Merkow* article"). The Applicants have thoroughly considered the Examiner's remarks concerning patentability of claim 9 over the *Easter* patent in view of the *Merkow* article. The Applicants have also thoroughly read the *Easter* patent and the *Merkow* article. As discussed in Section B above, the Applicants assert that the *Easter* patent fails to disclose, teach, or suggest an article of manufacture wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship, as recited in independent claim 6. The *Merkow* article also fails to disclose, teach, or suggest the same. Claim 9 depends indirectly from independent claim 6 and so includes all the elements and limitations of the respective independent claim 6 and intervening claims 7 and 8. The Applicants respectfully submit that dependent claim 9 is allowable over the *Easter* patent and the *Merkow* article for at least the same reasons as set forth above with respect to independent claim 6 and dependent claims 7 and 8.

Withdrawal of the rejection of claim 9 under 35 U.S.C. §103(a), as being unpatentable over the *Easter* patent in view of the *Merkow* article is respectfully requested.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 21 of 27

- E. Claims 11, 14, and 17 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold*.

As discussed in Section C above, the *Arnold* patent fails to disclose, teach, or suggest a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including the embedded client private key being associated with a client public key stored exclusively outside the read-only memory structure, as recited in amended independent claims 10, 13, or 16, respectively. Claims 11, 14, and 17 depend upon amended independent claims 10, 13, and 16, respectively, and include all the elements and limitations of their respective amended independent claims. Therefore, the *Arnold* patent fails to disclose all the limitations of the rejected claims. Claims 11, 14, and 17 are allowable for at least the reasons discussed above for their respective amended independent claims. Withdrawal of the rejection of claims 11, 14, and 17 under 35 U.S.C. §103(a) is respectfully requested.

- F. Claims 12, 15, and 18 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold* in view of U.S. Patent No. 5,559,889 to Easter *et al.*

As discussed in Section C above, the *Arnold* patent fails to disclose, teach, or suggest a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including the embedded client private key being associated with a client public key stored exclusively outside the read-only memory structure, as recited in amended independent claims 10, 13, or 16, respectively.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 22 of 27

The *Easter* patent fails to disclose, teach, or suggest a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including read-only memory structure having the embedded server public key, or the embedded server public key and the embedded client private key not being related by a cryptographic key pair relationship, as recited in amended independent claims 10, 13, or 16, respectively.

The *Easter* patent discloses designating a private key/public key pair for the IC chip. Fuse array 51 is encoded with the private key. Further, the fuse array is encoded with the hash value for the corresponding public key and a serial number. See column 5, lines 39-44. The public cryptographic key and the private cryptographic key in the *Easter* patent are related by a cryptographic key pair relationship. See column 5, lines 39-40.

Claims 12, 15, and 18 depend indirectly upon amended independent claims 10, 13, and 16, respectively, and include all the elements and limitations of their respective amended independent claims. Therefore, the *Arnold* and *Easter* patents, alone or in combination, fail to disclose all the limitations of the rejected claims. Claims 12, 15, and 18 are allowable for at least the reasons discussed above for their respective amended independent claims. Withdrawal of the rejection of claims 12, 15, and 18 under 35 U.S.C. §103(a) is respectfully requested.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 23 of 27

G. Claims 19-24 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold*.

The Applicants assert that the *Arnold* patent fails to disclose, teach, or suggest method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including the client public key is stored exclusively outside the client, as recited in amended independent claims 19, 21, and 23, respectively.

The *Arnold* patent discloses providing the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit. See column 4, lines 18-27. The *Arnold* patent fails to disclose storing the client public key exclusively outside the client, and so fails to teach or suggest all the claim limitations as recited in amended independent claims 19, 21, and 23, as required to sustain the rejection. Withdrawal of the rejection of claims 19, 21, and 23 under 35 U.S.C. §103(a) is respectfully requested.

Claims 20, 22, and 24 depend directly upon amended independent claims 19, 21, and 23, respectively, and include all the elements and limitations of their respective amended independent claims. Therefore, the *Arnold* and *Easter* patents, alone or in combination, fail to disclose all the limitations of the rejected claims. Claims 20, 22, and 24 are allowable for at least the reasons discussed above for their respective amended independent claims. Withdrawal of the rejection of claims 20, 22, and 24 under 35 U.S.C. §103(a) is respectfully requested.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 24 of 27

- H. Claims 25-30 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold* in view of U.S. Patent No. 5,559,889 to Easter *et al.*

The Applicants assert that the *Arnold* patent fails to disclose, teach, or suggest method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including the client public key stored exclusively outside the client, as recited in amended independent claims 25, 27, and 29, respectively.

The *Arnold* patent discloses providing the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit. *See* column 4, lines 18-27. The *Arnold* patent fails to disclose storing the client public key exclusively outside the client, and so fails to teach or suggest all the claim limitations as recited in amended independent claims 25, 27, and 29, as required to sustain the rejection.

The *Easter* patent fails to disclose, teach, or suggest a method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including read-only memory structure having the embedded server public key, or the embedded server public key and the embedded client private key not being related by a cryptographic key pair relationship, as recited in amended independent claims 25, 27, or 29, respectively.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 25 of 27

The *Easter* patent discloses designating a private key/public key pair for the IC chip. Fuse array 51 is encoded with the private key. Further, the fuse array is encoded with the hash value for the corresponding public key and a serial number. See column 5, lines 39-44. The public cryptographic key and the private cryptographic key in the *Easter* patent are related by a cryptographic key pair relationship. See column 5, lines 39-40.

The *Arnold* and *Easter* patents, alone or in combination, fail to disclose all the limitations of the rejected claims. Withdrawal of the rejection of claims 25, 27, and 29 under 35 U.S.C. §103(a) is respectfully requested.

Claims 26, 28, and 30 depend directly upon amended independent claims 25, 27, and 29, respectively, and include all the elements and limitations of their respective amended independent claims. Therefore, the *Arnold* and *Easter* patents, alone or in combination, fail to disclose all the limitations of the rejected claims. Claims 26, 28, and 30 are allowable for at least the reasons discussed above for their respective amended independent claims. Withdrawal of the rejection of claims 26, 28, and 30 under 35 U.S.C. §103(a) is respectfully requested.

I. Claims 31-39 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to *Arnold*.

The Applicants assert that the *Arnold* patent fails to disclose, teach, or suggest method, apparatus, or computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server in a data processing system including an embedded client private key being associated with a client public key stored exclusively outside the client, as recited in amended independent claims 31, 34, and 37, respectively.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 26 of 27

The *Arnold* patent discloses providing the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit. *See* column 4, lines 18-27. The *Arnold* patent fails to disclose storing the client public key exclusively outside the client, and so fails to teach or suggest all the claim limitations as recited in amended independent claims 31, 34, and 37, as required to sustain the rejection. Withdrawal of the rejection of claims 31, 34, and 37 under 35 U.S.C. §103(a) is respectfully requested.

Claims 32 and 33, claims 35 and 36, and claims 38 and 39 depend directly or indirectly upon amended independent claims 31, 34, and 37, respectively, and include all the elements and limitations of their respective amended independent claims. Therefore, the *Arnold* and *Easter* patents, alone or in combination, fail to disclose all the limitations of the rejected claims. Claims 32, 33, 35, 36, 38, and 39 are allowable for at least the reasons discussed above for their respective amended independent claims. Withdrawal of the rejection of claims 32, 33, 35, 36, 38, and 39 under 35 U.S.C. §103(a) is respectfully requested.

November 3, 2005
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 27 of 27

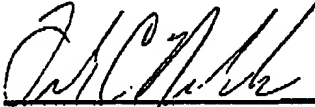
Summary

Reconsideration of claims 1-39 as amended is respectfully requested in light of the remarks herein. The Applicants submit that claims 1-39 as set forth by this Amendment fully satisfy the requirements of 35 U.S.C. §§ 102, 103, and 112. In view of foregoing remarks, favorable consideration and early passage to issue of the present application are respectfully requested.

Dated: November 3, 2005

Respectfully submitted,
David J. Craft, et al

CARDINAL LAW GROUP
1603 Orrington Avenue, Suite 2000
Evanston, IL 60201
(847) 905-7111



Frank C. Nicholas
Registration No. (33,983)
Attorney for Applicants